



DEPARTMENT OF THE NAVY

NAVAL HOSPITAL

BOX 788250

MARINE CORPS AIR GROUND COMBAT CENTER

TWENTYNINE PALMS, CALIFORNIA 92278-8250

IN REPLY REFER TO:

NAVHOSP29PALMSINST 5239.1

Code 0130

26 August 1997

NAVAL HOSPITAL TWENTYNINE PALMS INSTRUCTION 5239.1

From: Commanding Officer, Naval Hospital Twentynine Palms

Subj: INFORMATION SYSTEM SECURITY (INFOSEC) PROGRAM

Ref: (a) SECNAVINST 5239.3

1. Purpose. To direct this command's INFOSEC program, per reference (a).

2. Scope. All command information systems (IS), networks, and computer resources must be protected. The policies defined in reference (a) apply to the command INFOSEC accreditation, life-cycle management, risk management, contingency planning, user access, security application, and the formal written appointment of INFOSEC staff. This instruction applies to command personnel, including contractors, who operate ISs, networks, printing and imaging equipment, systems that are part of an IS, and any other systems, whether local or remote, for which this command is responsible. This includes joint services, other Department of Navy (DoN) ISs, and ISs resources operated but not owned by this command, when security requirements have not been specified.

3. Program Elements. Per reference (a), the command INFOSEC program will contain the following elements:

a. All operating IS equipment will be accredited or have an interim authority to operate.

b. The Chief, Bureau of Medicine and Surgery will approve, in writing, the authority to process classified information on any IS equipment or any network after certification by Naval Criminal Investigative Service and Naval Electronic Security Systems Engineering Command.

c. Classified, privacy act, and sensitive data will be protected.

4. Responsibilities

a. The Commanding Officer (CO) is responsible for certifying that all systems meet and maintain prescribed security requirements and standards. The Officer in Charge (OIC) of each command detachment is responsible for determining that the systems at their assigned detachment meet and maintain all security requirements and standards. The CO has the final systems certification authority.

NAVHOSP29PALMSINST 5239.1
26 August 1997

b. The CO will appoint in writing a Security Manager (SM) who serves as the Special Assistant for INFOSEC.

c. The SM will:

(1) Facilitate the backup of all critical files and provide for off-site storage. Directors will work closely with the SM to identify all critical files.

(2) Test the command contingency plan, ensuring that any contingencies do not impede the information processing capability under the authority of this command.

(3) Ensure procedures are in place to safeguard data from loss, corruption, or malicious destruction.

d. Information Systems Security Manager (ISSM) is appointed by the CO and advises the SM on all INFOSEC matters and is the command's point of contact (POC). The ISSM will:

(1) Develop and submit an organizational Activity INFOSEC Plan/Activity Accreditation Schedule (AIP/AAS); complete a risk assessment; install appropriate and effective countermeasures; and, develop and test the command's Security Test and Evaluation Plan and Contingency Plan.

e. Network Security Officer (NSO) is appointed by the CO and is responsible to the ISSM for implementing, maintaining, and enforcing network security requirements. The NSO is the POC for network security issues. The NSO issues network security requirements, reviews network configuration changes, works closely with ISSOs, and coordinates the submission of accreditation documentation with the ISSM. The NSO ensures that security is provided throughout the local area network (LAN) and its components.

f. Information Systems Security Officer (ISSO). Each Director and OIC will select ISSOs and the CO will appoint the selected individuals. ISSOs ensure that security is provided for and implemented throughout the life cycle of an information resource and implementing system in the operational environment. ISSOs will:

(1) Serve as the POC for all Directorate INFOSEC matters.

(2) Execute the INFOSEC program as it applies to the assigned ISSs including preparing and submitting supporting documentation for the command's Accreditation package.

(3) Maintain an inventory of IS hardware, system software releases, and major functional application systems.

(4) Monitor IS activity, including identification of the levels and types of data handled; assign passwords; and, review audit trails and outputs to ensure compliance with INFOSEC directives and procedures.

(5) Conduct and document a risk assessment of IS resources. Develop and annually test contingency plans. Contribute to the INFOSEC IS plans.

(6) Supervise, test, and monitor changes in the ISs affecting the command and network INFOSEC program.

(7) Maintain a list of authorized users for each IS ensuring an audit trail is kept for system access.

(8) At regular intervals scan systems for computer virus infections and report any infections to the ISSM.

(9) Provide INFOSEC awareness training in assigned area of responsibility.

(10) Assist the ISSM with the INFOSEC program.

(11) Monitor IS procurements for security impact to ensure compliance with security regulations and known security requirements.

g. The Terminal Area Security Officer (TASO). Each Director and OIC will select TASOs and the CO will appoint the selected individuals. The TASO assists the ISSM and ISSO with the INFOSEC program as it relates to assigned terminals within a specific environment. TASOs will:

(1) Ensure that INFOSEC requirements and countermeasures issued by the ISSO to protect IS equipment are in place and operating effectively. This includes use of passwords for system access, list of authorized users for each system, an audit trail, scanning systems for computer viruses at regular intervals, and reporting any computer virus infections.

(2) Work closely with the ISSO, making recommendations for improved terminal area security and the maintenance of a high level of INFOSEC security awareness. Provide assistance to ensure continued security for command terminal areas.

(3) Brief and indoctrinate each terminal user on security policies and procedures before their access to the system.


(4) Establish and maintain a current list of all authorized terminal users to include name, code, security clearance, and terminal and user identification codes.

NAVHOSP29PALMSINST 5239.1
26 August 1997

(5) Provide the ISSO with a copy of the access list upon initial installation of a terminal.

(6) Notify the ISSO of sensitive but unclassified data (Privacy Act, For Official Use Only, sensitive business, financial, and personnel) received that cannot be identified, contains extraneous data, or is an unrequested output.

(7) Participate in risk assessments, contingency plan testing, and security test and evaluation plan development, as required.



R. S. KAYLER

Distribution:
List A